MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2022/2023 (TERM ID 2210)

TAC3121 – APPLIED CRYPTOGRAPHY

(All sections / Groups)

7 FEBRUARY 2023
2.30 p.m. – 4.30 p.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 3 pages including the cover page with **FIVE** questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1

(a) Define Kerchoffs' Principle? [2 marks]

(b) State Euler's Theorem, and use it to compute 7^{101} mod 12. [5 marks]

(c) What is a hash function? Define the property of Preimage Resistant for a secure hash function. [3 marks]

Question 2

(a) Assuming you can do 2^{30} decryptions per second and the key size is 56 bits, how long would a brute force attack take? (state in days) [3 marks]

(b) Decrypt the following ciphertext using Caesar cipher with key $K = 5$:

LT FKYJW DTZW IWJFR [3 marks]

(c) Decrypt the following ciphertext using the 2-row Rail Fence cipher:
GETIDDSUSDARAMNSICSIES [4 marks]

Question 3

Given the following RSA parameters: primes, $p = 17$, $q = 3$; exponent, $e = 5$.

(a) Can the exponent, $e = 2$ be used in RSA? Justify your answer. [2 marks]

(b) Demonstrate that $e = 5$ is a valid RSA exponent. [3 marks]

(c) Using the given RSA parameters, compute the private key d. [3 marks]

(d) Next, decrypt the ciphertext, $c = 15$. [2 marks]

Continued...

Question 4

(a) State the outputs of the DES S-box S_2 given the inputs 110011 and 011001 respectively.

S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

[4 marks]

(b) How many keys are used in 3DES? Why is the middle portion of 3DES a decryption rather than an encryption? [4 marks]

(c) In Cipher Block Chaining (CBC) mode of DES, if there is a bit error in the plaintext block P_1 during encryption, through how many ciphertext blocks is this error propagated? Justify your answer. [2 marks]

Question 5

(a) List and explain the THREE (3) adversarial capabilities and the THREE (3) adversarial goals for a digital signature scheme. Which combination provides the most desirable security notion upon comparison? [4 marks]

(b) A digital signature and a message authentication code (MAC) both provide data integrity. What is the additional security goal which can be provided by a digital signature but not by a MAC? Why not? [3 marks]

(c) Diffie-Hellman key exchange is vulnerable to the man-in-the-middle attack. Suggest a solution to overcome this vulnerability and explain your answer. [3 marks]

End of Page